

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Middesk, Inc.

Plaintiff,

v.

Osiris Ratings, Inc. d/b/a Baselayer, and

**Jonathan Awad, and
Josh Levloff,**

Defendants.

CIVIL ACTION NO. 1:25-CV-02677

Jury Trial Demanded

**PLAINTIFF'S MEMORANDUM OF LAW IN SUPPORT OF
ORDER TO SHOW CAUSE FOR EXPEDITED DISCOVERY**

OF COUNSEL:

GREENBERG TRAURIG, LLP
Justin K. Victor (*phv forthcoming*)
Fredric J. Bold, Jr. (*phv forthcoming*)
Rushton Pope (*phv forthcoming*)
3333 Piedmont Road NE, Suite 2500
Atlanta, GA 30305
(678) 553-2100
victorj@gtlaw.com
rick.bold@gtlaw.com
rushton.pope@gtlaw.com

Dated: March 31, 2025

GREENBERG TRAURIG, LLP
Jason D. Burns
Shira M. Poliak
One Vanderbilt Avenue
New York, NY 10017
(212) 801-9294
Jason.Burns@gtlaw.com
Shira.Poliak@gtlaw.com

Counsel for Plaintiff Middesk, Inc.

TABLE OF CONTENTS

I.	STATEMENT OF FACTS.....	2
A.	Background.....	2
B.	Middesk Employed Awad Before He Left to Form Middesk's Competitor Baselayer Using Middesk's Confidential Information.....	4
C.	Awad Convinces Middesk Employee Leviloff to Steal Additional Confidential Information and Trade Secrets in January 2025 Before Leviloff Leaves for Baselayer.....	4
D.	Leviloff Downloads Sensitive Data about Middesk's Products.....	7
E.	Leviloff Accesses and Obtains Sensitive Data from Salesforce Without a Valid Business Purpose.....	8
F.	Leviloff Attempts to Leave Middesk with No Trace While Maintaining Access to Confidential Middesk Data on his Personal Device.....	9
G.	Middesk's IT Forensics Expert Amassed Evidence of Defendants' Misconduct and Identified the Devices and Data Sources in Defendants' Exclusive Possession.....	10
II.	ARGUMENT.....	11
A.	The Evidence of Defendants' Misconduct Easily Constitutes Good Cause for Expedited Discovery.....	13
B.	Even Though the Court Need Not Consider Them, the <i>Notaro</i> Factors Also All Weigh in Favor of Granting Middesk's Motion.....	14
C.	The Expedited Discovery Middesk Seeks is Reasonable and Tailored.....	17
1.	Middesk Seeks a Small Number of Document Requests, Interrogatories, and Depositions.....	17
2.	Middesk Seeks a Forensic Examination of Specifically Identified Devices/Sources.....	19
III.	CONCLUSION.....	22

TABLE OF AUTHORITIES

	Page(s)
<i>Ayyash v. Bank Al-Madina,</i> 233 F.R.D. 325 (S.D.N.Y. 2005)	12, 13, 14
<i>Campbell Alliance Grp., Inc. v. Dandekar,</i> No. 13-415, 2013 WL 12144048 (E.D.N.C. Dec. 23, 2013)	20
<i>Ceglia v. Zuckerberg,</i> No. 10-569, 2013 WL 1208558 (W.D.N.Y. March 26, 2013)	20
<i>Citibank, N.A. v. Mitchell,</i> No. 24-8224, 2024 WL 4906076 (N.D. Cal. Nov. 26, 2024)	20
<i>Comet Techs. United States of Am. Inc. v. Beuerman,</i> No. 18-1441-LHK, 2018 WL 1990226 (N.D. Cal. Mar. 15, 2018)	21
<i>Crawford-El v. Britton,</i> 523 U.S. 574 (1998)	11
<i>Digital Sin, Inc. v. Does 1-176,</i> 279 F.R.D. 239 (S.D.N.Y. 2012)	12
<i>Estee Lauder Cos. v. Batra,</i> 430 F. Supp. 2d 158 (S.D.N.Y. 2006)	15
<i>FMC Corp. v. Taiwan Giant Indus. Co.,</i> 730 F.2d 61 (2d Cir. 1984)	14, 15
<i>IKON Office Solutions, Inc. v. Leichtnam,</i> No. 02-721, 2003 WL 251954 (W.D.N.Y. Jan. 3, 2003)	16
<i>IME Watchdog, Inc. v. Safa Abdulrahim Gelardi, et. al.,</i> No. 22-cv-1032 (E.D.N.Y. May 13, 2022)	20
<i>In re Keurig Green Mountain Single-Serve Coffee Antitrust Litig.,</i> No. 14-4242, 2014 WL 12959675 (S.D.N.Y. July 23, 2014)	12
<i>Nebraskaland, Inc. v. Brody,</i> No. 09-9155, 2010 WL 157496 (S.D.N.Y. Jan. 13, 2010)	13
<i>North Atlantic Operating Co. v. Evergreen Distributors, LLC,</i> 293 F.R.D. 363 (E.D.N.Y. 2013)	16
<i>Notaro v. Koch,</i> 95 F.R.D. 403 (S.D.N.Y. 1982)	12

<i>PLC Trenching Co., LLC v. Newton,</i> No. 11-515, 2011 WL 13135653 (N.D.N.Y. 2011).....	20
<i>Pyro Spectaculars North, Inc. v. Souza,</i> No. 12-299, 2012 WL 13220023 (E.D. Cal. Feb. 8, 2012).....	20
<i>R.R. Donnelley & Sons Co. v. Marino,</i> 505 F. Supp. 3d 194 (W.D.N.Y. 2020).....	17
<i>Russell Reynolds Assocs., Inc. v. Usina,</i> No. 23-2369, 2023 WL 3270344 (S.D.N.Y. May 5, 2023)	12, 17
<i>Sapient Corp. v. Singh,</i> 149 F. Supp. 2d 55 (S.D.N.Y. 2001).....	16
<i>Stern v. Cosby,</i> 246 F.R.D. 453 (S.D.N.Y. 2007)	12, 14
<i>Suber v. VVP Servs.,</i> No. 20-8177, 2021 WL 1101235 (S.D.N.Y. Mar. 23, 2021).....	14
<i>Synopsys, Inc. v. InnoGrit, Corp.,</i> No. 19-2082, 2019 WL 1779978 (N.D. Cal. Apr. 23, 2019).....	20
<i>Uni-World Capital L.P. v. Preferred Fragrance, Inc.,</i> 73 F. Supp. 3d 209 (S.D.N.Y. 2014).....	12

Rules

Fed. R. Civ. P. 26.....	11
-------------------------	----

Plaintiff Middesk, Inc. moves the Court on an emergency basis for narrow expedited discovery because it has hard evidence of a brazen theft of its trade secrets coordinated by the CEO of Middesk's business competitor, Defendant Baselayer. Smoking-gun text messages confirm that Defendant Jonathan Awad, Baselayer's CEO, instructed Middesk's then-employee Defendant Josh Leviloff to obtain and transmit highly sensitive business documents—including by lying about why Leviloff needed those documents—right before Leviloff left Middesk to join Baselayer. Leviloff then tried to cover his tracks, including by researching how to “Delete your Google Account.”

Given this shocking intrusion into the heart of Middesk's business by a competitor, Middesk needs early, narrow expedited discovery to preserve the status quo of the evidentiary record and so the Court can consider Middesk's forthcoming motion for a preliminary injunction with a fair factual record. While Middesk possesses ample facts substantiating Defendants' scheme and theft of trade secrets, including a detailed report from Middesk's IT forensics expert, Middesk does not possess or have access to all the devices / data sources that would show the full extent of what Defendants took, where they disseminated it and how they have been using it. That is why Middesk needs the Court's compulsory discovery process at the outset of this case on an emergency basis.

Middesk's request for expedited discovery is narrow, critical, and supported by evidence from Middesk's forensic IT expert. Middesk needs expedited discovery so it can move for a preliminary injunction on a complete and fair record and so the Court can confirm the extent of what Defendants have stolen, where it went, and how Middesk has been harmed. Middesk seeks (i) responses to a limited number of document requests and interrogatories, (ii) a Court-ordered forensic imaging of the devices/data sources identified by Middesk's forensics expert, and (iii) a

deposition of three hours or less of each defendant. The Court uses just a “good cause” standard to order expedited discovery in its discretion. Under these extraordinary facts and given the parties’ competing businesses, Middesk’s emergency motion is warranted and reasonable. Given that the confidential information and trade secrets at issue are Middesk’s own data and that Defendants had no right to obtain or use that information outside of ordinary Middesk employment, there is no harm to Defendants. And while Middesk has done everything it can to gather evidence about this scheme, Middesk needs this Court’s compulsory discovery tools to complete that investigation into Defendants’ theft and ongoing breaches. The devices/data sources Middesk seeks are uniquely in Defendants’ control, and Middesk’s IT forensics expert has identified, with evidence, the precise devices/data sources that likely contain Middesk’s confidential information and trade secrets but to which Middesk does not have access.

In addition to ordering this expedited discovery, Middesk requests that the Court issue an Order to Show Cause that sets a schedule for the parties to complete the expedited discovery, to schedule briefing for Middesk’s requested preliminary injunction, and to set a preliminary injunction hearing date.

For the following reasons, the Court should grant Middesk’s Motion.

I. **STATEMENT OF FACTS¹**

A. Background

This is a case about the calculated theft of Middesk Inc.’s (“Middesk”) trade secrets, proprietary, and confidential information. The theft was orchestrated by a former Middesk employee, Defendant Jonathan Awad, who is now the Chief Executive Officer and founder of Defendant Osiris Ratings, Inc. d/b/a Baselayer (“Baselayer”). Complaint [ECF No. 1] (“Compl.”)

¹ Plaintiff’s Verified Complaint is filed contemporaneously with this motion. Plaintiff incorporates by reference all facts and allegations set forth in the Verified Complaint.

¶ 1. Through computer forensics, it has become apparent that Awad is desperate to unlawfully replicate Middesk's product and service offerings at Baselayer. *Id.*

Incorporated in 2018, Middesk is a leading provider of business verification, credit assessment, and entity management products. *Id.* ¶ 16. Among other services, Middesk helps its customers verify the legitimacy, health, and history of small businesses; Middesk provides these services through proprietary tools that efficiently and accurately search, synthesize, and analyze massive volumes of data. *Id.* More than 500 customers in the fintech, banking, lending, marketplace, insurance, and payroll sectors trust Middesk to help them safely verify and underwrite their small- or medium-sized business customers. *Id.* ¶ 2.

Middesk has invested substantial resources, both financially and in human capital, to develop the trade secrets and other confidential and proprietary information stolen and misappropriated by Defendants. *Id.* ¶ 17. It has taken Middesk multiple years, thousands of people hours, and millions of dollars to build out the data infrastructure, vendor relationships, and technology that power Middesk's products and that have helped Middesk to become a market leader. *Id.* ¶ 18.

Among the confidential information that Defendants stole from Middesk is information about which data providers Middesk uses for certain products. *Id.* Middesk employs a comprehensive, data-driven methodology to evaluate and select optimal data vendors for each of its products; this selection process incorporates proprietary data accumulated over multiple years, which Middesk leverages to refine its product partner selection, differentiate its products in the market, and optimize service delivery to customers. *Id.* This non-public data would otherwise be very difficult for competitors and new entrants to the market to learn. *Id.* Further, Middesk has made substantial investments in securing preferential commercial terms and pricing structures with

these data partners, creating significant competitive advantages and adding value for its customers.

Id.

As detailed in the Complaint, Middesk has taken appropriate steps to protect the confidentiality of its information. *Id.* ¶ 20.

B. Middesk Employed Awad before He Left to Form Middesk's Competitor Baselayer Using Middesk's Confidential Information.

Awad worked at Middesk as an Account Executive and then a Partnerships Manager from June 2021 to January 2023 and had access to Middesk's confidential and proprietary information, including pricing and pipeline plans. *Id.* ¶ 21-23. Awad was bound by a Proprietary Information and Inventions Agreement (the "Awad Agreement") in which he promised to "hold in confidence and not disclose or, except within the scope [of his employment] use any Proprietary Information" and to return all Middesk proprietary information upon his employment's termination. *Id.* ¶ 24-25.

Between October 2022 and his termination in January 2023, Awad used his Middesk email address to forward confidential, proprietary and trade secret information about Middesk's business to his personal email address. *Id.* ¶ 28. These documents included, *inter alia*, information about internal pricing and product strategy for Middesk's lien search product, product-launch plans, product strategy and growth plans, and spreadsheets containing the contact information for hundreds of potential customers. *Id.* Middesk believes that Awad improperly used this information that he took in violation of the Awad Agreement to build his competing business Baselayer. *Id.* ¶ 29-30. Awad incorporated Baselayer less than one month after his termination and has continued to reach out to Middesk employees fishing for information about the company. *Id.* ¶ 31-33.

C. Awad Convinces Middesk Employee Leviloff to Steal Additional confidential Information and Trade Secrets in January 2025 before Leviloff Leaves for Baselayer.

Leviloff worked at Middesk as an Account Executive from July 2023 to February 21, 2025 and had access to Middesk's confidential and proprietary information. *Id.* ¶ 35. Leviloff was likewise bound by a Proprietary Information and Inventions Agreement (the "Leviloff Agreement"), which included obligations to keep Middesk's information confidential and to return all proprietary information upon termination. *Id.* ¶ 37-38. The Leviloff Agreement also included an obligation not to compete or prepare to compete with Middesk or to assist anyone else in competing or preparing to compete. *Id.* ¶ 39.

Computer forensics have confirmed that, as of January 22, 2025, Awad and Leviloff had extensive communications whereby Awad recruited Leviloff to leave Middesk and join Baselayer. *Id.* ¶ 42. By no later than February 1, 2025, Leviloff had executed an employment contract with Baselayer. *Id.* ¶ 43. On February 2, 2025, Awad instructed Leviloff **not** to sign a termination agreement with Middesk and told him that there was "no need to rush telling [Middesk] where you're going right away... the LinkedIn update will be very fun." *Id.* ¶ 44. It would obviously be harder for Leviloff to steal Middesk's confidential information if Middesk knew Leviloff was imminently leaving for Baselayer.

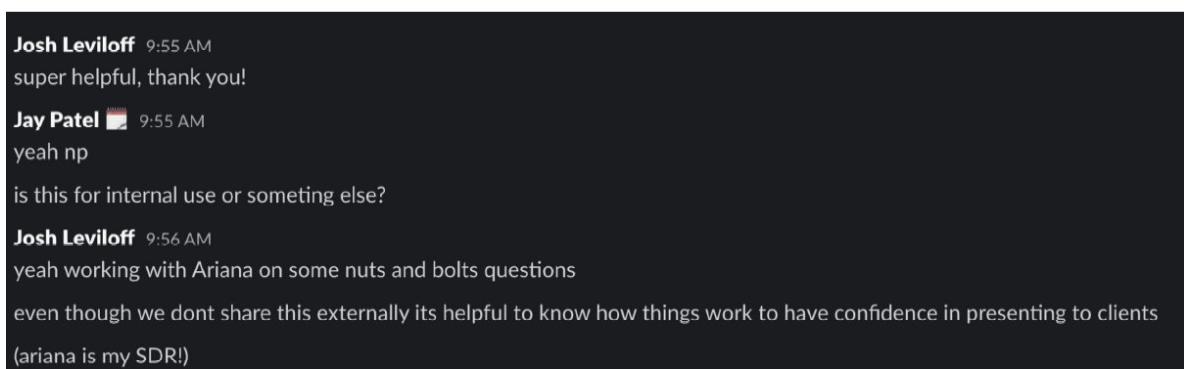
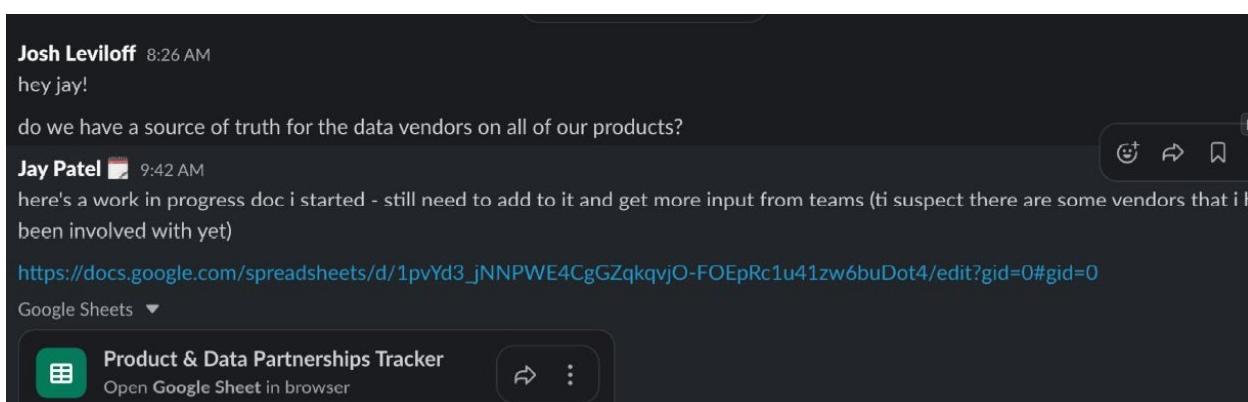
On February 4, 2025, Awad directed Leviloff in a text message to access and share Middesk's confidential and proprietary information with Awad and Baselayer. *Id.* ¶ 46.

Awad directed Leviloff to determine what vendors Middesk uses to provide certain services and directed Leviloff to "[a]sk around and validate this [list] with anyone in [Middesk] product before you head out." *Id.* ¶ 47. Leviloff responded that he planned to ask for the information, to which Awad responded that he was grateful—"Amazing sir ty [thank you]." *Id.* ¶ 48.

All of the services that Awad instructed Leviloff to investigate at Middesk are services that Baselayer also provides in competition with Middesk. *Id.* ¶ 49.

On February 10, 2025, Leviloff complied and asked for a “source of truth for the data vendors on all of [Middesk’s] products.” *Id.* ¶ 50. The document containing the information Awad directed Leviloff to gather (and more) is called the Product & Data Partnerships Tracker. *Id.* That document lists: (a) all of Middesk’s product and data vendors; (b) what each vendor manages for Middesk; (c) what products Middesk purchased from each vendor; and (d) internal notes, including potential future negotiation strategies with specific vendors. *Id.*

Leviloff did not ordinarily have access to this document and when asked by Middesk’s Product Partnerships Lead why he needed the document and whether it was for “internal use or something else,” Leviloff lied. *Id.* ¶¶ 51-52. Leviloff told the Product Partnerships Lead he was working on some “nuts and bolts” questions. *Id.* at ¶ 52. When the Product Partnerships Lead asked Leviloff if this was for internal Middesk use, Leviloff lied again and said, “yeah … even though we dont [sic] share this externally its [sic] helpful to know how things work to have confidence in presenting to clients.” *Id.* ¶ 52.



After Leviloff obtained the Product & Data Partnerships Tracker and before he was terminated, Leviloff synced that document to a non-Middesk device, which Middesk believes he did so he could use the document at Baselayer. *Id.* ¶ 53.

On February 11, 2025, just one day after obtaining access to the information Awad had directed him to uncover, Leviloff informed Middesk that he would be resigning and that his last day would be February 21, 2025. *Id.* ¶ 56. Leviloff was allowed to continue working for Middesk because he informed his manager that he had been accepted into a Master of Business Administration (“MBA”) program, and that he was resigning because he intended to go back to school in the Fall of 20205. *Id.* At the time, Leviloff did not disclose to Middesk that he had in fact been in conversation with Awad and that he intended to work at Baselayer. *Id.*

D. Leviloff Downloads Sensitive Data about Middesk’s Products.

Unfortunately, this brazen example of misappropriation by Leviloff on Awad’s and Baselayer’s behalf was just the beginning.

On February 19, 2025, logs for the Company’s Google Workplace account, a secure password-protected cloud computing document and email platform, show that Leviloff accessed and downloaded a file titled “Middesk Model Validation.” *Id.* ¶ 57. Leviloff performed this download using a device that was not issued by the Company. *Id.*

The Middesk Model Validation document outlines Middesk’s approach to developing models for matching the names of people and companies against global sanctions lists and ensuring that the returned results meet the quality and performance expectations of enterprise financial

service firms and the federal regulators with whom those people and companies work. *Id.* ¶ 58. Middesk worked with an external firm to develop, validate, and test various solutions to developing this model in a way that would support their compliance programs. *Id.* Middesk shares this with customers only under an NDA. *Id.* Middesk believes that Awad and Baselayer have gained access to the information within the Middesk Model Validation and are using, or plan to use, that information to compete with Middesk. *Id.* ¶ 59. Middesk's access logs also show suspicious patterns in the internal documents that Leviloff was accessing, starting at the same time Leviloff and Awad began discussing Leviloff joining Baselayer. *Id.* ¶ 60. For example, there are numerous confidential documents that Leviloff had not accessed a single time in his year and a half working at Middesk but that he accessed dozens of times in his last few weeks. *Id.* That is strong evidence that Leviloff accessed these documents at Awad's and Baselayer's direction and/or with the intention of sharing them with Awad and Baselayer.

E. **Leviloff Accesses and Obtains Sensitive Data from Salesforce Without a Valid Business Purpose.**

Further, *after Leviloff had executed his employment agreement with Baselayer in February 2025*, including late on his last day employed at Middesk, Leviloff's account was used to access Middesk's Salesforce portal. *Id.* ¶ 61. Salesforce is a password-protected database that contains highly confidential sales information, including pricing, and summaries of discussions with key customer contacts. *Id.* Middesk employees are not permitted to share Salesforce passwords with third-parties. *Id.*

Leviloff texted Awad on February 1, 2024 that he signed his offer letter. *Id.* ¶ 62. He added that he is “going to be in [V]ail with [his] girlfriend and her family this week, so [] might be slow to respond but I’m absolutely PSYCHED.” *Id.* But despite being on vacation, on February 3 and 4, Leviloff successfully logged in to Salesforce from Avon, Colorado, a short distance from Vail.

Id. ¶ 63. Over the next approximately two weeks, Leviloff continued to sign into Salesforce throughout his travels in the U.S., including in Ashburn, Virginia; Boardman, Oregon; and most frequently from New York, New York and accessed Salesforce a number of times from his phone and a Baselayer or personal device. *Id.* ¶ 64. These odd facts strongly suggest that Leviloff used that information for the benefit of Awad and/or Baselayer, but without access to Leviloff's personal devices and cloud storage, Middesk cannot ascertain the extent of the information he obtained and how he may have used or shared it. *Id.* ¶ 65.

F. Leviloff Attempts to Leave Middesk with No Trace While Maintaining Access to Confidential Middesk Data on his Personal Device.

Leviloff's last day at Middesk was February 21, 2025. *Id.* ¶ 66. Notably, at 12:56 pm that day, Leviloff deliberately cleared the internet browser history on his Middesk-provided laptop, and accessed a link with the title "**Delete your Google Account.**" *Id.* But as late as his last day, Leviloff continued to access Middesk's Salesforce portal from his personal iPhone, even though there was no legitimate business purpose to do that on his last day of employment. *Id.* ¶ 67.

Even more concerning, Middesk has evidence that Leviloff used a personal email account with the ability to access an Apple iCloud feature to synchronize data between a device and cloud storage. *Id.* ¶ 68. Middesk's preliminary IT forensics indicates that Leviloff enabled an Apple iCloud Drive while using his work computer, which means that Leviloff accessed and saved Middesk's trade secrets onto a personal device on his last day of employment. *Id.*

Middesk's forensic analysis has also confirmed that on February 20, 2025, Leviloff's next-to-last day at Middesk, Leviloff synchronized (and therefore copied) thirty-eight files from Middesk's password-protected Google drive. *Id.* ¶ 69. This is particularly concerning because there is no evidence that any of these files were copied to Defendant Leviloff's Middesk laptop; in other words, Leviloff copied these files onto a personal device or a Baselayer device. *Id.* Importantly,

Leviloff had not accessed some of those documents for over a month yet the documents included confidential and sensitive trade secrets. *Id.* ¶ 70. For example, some of these documents contain pricing and volume pricing information for all Middesk's products and an internal model that Middesk built to help with sales and explain the value of Middesk's products; other documents outline feedback that Middesk has received on its products, something that Leviloff would have had no legitimate business use for in his final days of employment.

G. Middesk's IT Forensics Expert Amassed Evidence of Defendants' Misconduct and Identified the Devices and Data Sources in Defendants' Exclusive Possession.

After Leviloff's departure, Middesk retained an IT forensics expert, Julian Ackert, Managing Director of iDiscovery Solutions in Washington, D.C., to analyze Leviloff's Middesk computer and activity logs. A declaration reflecting Ackert's findings is attached as Exhibit C to Middesk's Complaint ("Ackert Decl."). Ackert forensically imaged Leviloff's Middesk laptop and analyzed that device combined with Leviloff's Google Drive logs, Salesforce login logs, and Slack messages. Decl. ¶¶ 19-21.

Ackert's summary of his opinions and findings based on his analysis to date include:

- Leviloff downloaded or synchronized at least 38 files from Middesk's Google Drive to a device other than his Middesk laptop, including files related to Middesk's pricing, business operations, and sales pipeline. *Id.* ¶ 9.
- Leviloff's Middesk laptop was used to access Leviloff's personal Gmail account as well as Middesk Salesforce pages related to Middesk's sales pipeline, pricing, and accounts. *Id.* ¶ 11.
- Leviloff accessed Middesk's Salesforce system from his iPhone between December 5, 2024 and February 21, 2025. *Id.* ¶ 12.
- While Middesk has some of the damning Awad-Leviloff text messages, Leviloff disconnected his personal text message database from his Middesk laptop on February 6, 2025. *Id.* ¶ 13.
- Leviloff's browsing history on his Middesk laptop was cleared on his last day of employment, limiting Ackert's ability to conduct a full forensic investigation. *Id.* ¶ 10.

Based on his analysis, Ackert also identified a list of devices and other data sources not in Middesk's possession that Ackert would need to complete his IT forensics investigation:

- Leviloff's Gmail account: jXXXXXXXXXX@gmail.com;
- Leviloff's iCloud account associated with the email address jXXXXXXXXXX@yahoo.com;
- Leviloff's personal phone;
- Leviloff's personal computer(s);
- Leviloff's Baselayer-provided computer;
- Leviloff's Baselayer-provided email account;
- Awad's Apple ID associated with email account j*****@gmail.com, including the full email address and password;
- Awad's device(s) used to communicate with Leviloff;
- Awad's Baselayer-provided computer;
- Awad's Baselayer-provided email account; and
- Baselayer accounts or systems that Leviloff connected to or emailed. *Id.* ¶ 65.

II. ARGUMENT

This Court can and should easily grant this Motion under the “flexible standard of reasonableness and good cause” that courts in this District routinely apply. Including through a recent brazen scheme directed by Baselayer’s CEO Awad, Awad and Leviloff have improperly obtained confidential information and trade secrets from Middesk in violation of their Middesk confidentiality agreements; Leviloff’s theft occurred just as Leviloff was leaving Middesk to join Baselayer. There is good cause for expedited discovery here to preserve the record evidence, enable Middesk to understand the full scope of Defendants’ violations, and to have a fair opportunity to review evidence that is otherwise unavailable to Middesk as it prepares for a preliminary injunction hearing.

Rule 26 affords the Court power and wide discretion to determine the timing and sequence of discovery. *See Crawford-El v. Britton*, 523 U.S. 574, 598 (1998) (affirming a Court’s “broad discretion” to tailor discovery and to “dictate the sequence of discovery”). More specifically, “[c]ourts in this district have applied a ‘**flexible standard of reasonableness and good cause**’ in

determining whether to grant a party’s expedited discovery request.” *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 241 (S.D.N.Y. 2012) (granting expedited discovery for “good cause,” including because movant had “no other way of obtaining” the information) (emphasis added). While a much older line of cases used a four-factor test from *Notaro v. Koch*, 95 F.R.D. 403, 405 (S.D.N.Y. 1982), to assess whether to allow expedited discovery, the more recent and better-reasoned decisions just apply the “more flexible ‘good cause’ test.” *Ayyash v. Bank Al-Madina*, 233 F.R.D. 325, 326-27 (S.D.N.Y. 2005) (highlighting that “the intention of the rule-maker was to confide the matter to the Court’s discretion, rather than to impose a specific and rather stringent test”); *see also In re Keurig Green Mountain Single-Serve Coffee Antitrust Litig.*, No. 14-4242, 2014 WL 12959675, at *1 (S.D.N.Y. July 23, 2014) (“[C]ourts in this District have shifted away from the *Notaro* test and moved towards a more flexible ‘good cause’ or ‘reasonableness’ standard”); *Stern v. Cosby*, 246 F.R.D. 453, 457 (S.D.N.Y. 2007) (same).²

Applying that lower good-cause standard is “especially” appropriate “when applied to a request to expedite discovery in order to prepare for a preliminary injunction hearing,” as here. *Ayyash*, 233 F.R.D. at 326-27; *see also Russell Reynolds Assocs., Inc. v. Usina*, No. 23-2369, 2023 WL 3270344, at *1 (S.D.N.Y. May 5, 2023) (“Requests for expedited discovery are typically appropriate where [the information sought] ‘would better enable the court to judge the parties’ interests and respective changes for success on the merits at a preliminary injunction hearing.’”).

This Court also frequently permits expedited discovery when the discovery sought is uniquely within the possession of the other party, also as here. *See, e.g., Uni-World Capital L.P.*

² The *Notaro* four factors are: “(1) irreparable injury, (2) some probability of success on the merits, (3) some connection between the expedited discovery and the avoidance of the irreparable injury, and (4) some evidence that the injury will result without expedited discovery looms greater than the injury that the defendant will suffer if the expedited relief is granted.” *Stern*, 246 F.R.D. at 457.

v. Preferred Fragrance, Inc., 73 F. Supp. 3d 209, 212 (S.D.N.Y. 2014) (expedited discovery granted in case alleging the violation of non-compete agreements); *NebraskaLand, Inc. v. Brody*, No. 09-9155, 2010 WL 157496, at *1 (S.D.N.Y. Jan. 13, 2010) (expedited discovery permitted in restrictive covenant case involving alleged solicitation of employees and customers).

A. The Evidence of Defendants' Misconduct Easily Constitutes Good Cause for Expedited Discovery.

Given the hard evidence about Defendants' theft of Middesk's confidential information and trade secrets to aid a competing business, the expedited discovery Middesk seeks here is reasonable based "on the entirety of the record to date" and "in light of all the surrounding circumstances." *Ayyash*, 233 F.R.D. at 327.

As set forth in detail *supra* at 2-11 and in the Verified Complaint at ¶¶1-70, expedited discovery is warranted due to the brazen, intrusive scheme that Baselayer's CEO Awad instigated with Leviloff immediately before Leviloff left Middesk to join Baselayer. For example, Awad instructed Leviloff to obtain and transmit highly sensitive information about Middesk's business and customers, that would be valuable to a direct competitor like Baselayer and would cause substantial damages to Middesk, including Middesk's Product & Data Partnerships Tracker. Knowing how valuable the Tracker was and that he had no legitimate reason to possess it, Leviloff lied to Middesk's Product Partnerships Lead saying he needed it for internal use in order to obtain it.

In addition, Google Workplace logs show that Leviloff used devices other than his Middesk laptop to download the Company's confidential information and to steal dozens of confidential Middesk documents using an external iCloud account in the days and hours before his departure. Leviloff tried to cover his tracks by attempting to delete his browser history, even going so far as

to search how to “Delete your Google Account.” The information that Leviloff stole took years for Middesk to refine and monetize. *See Compl.* ¶ 18.

All that happened after Awad himself improperly emailed confidential and proprietary Middesk information to his personal email address when still employed by Middesk, including strategy documents and customer pipeline information right before establishing Baselayer to directly compete with Middesk. *See Compl.* ¶¶ 3, 8, 28.

This is strong evidence of Middesk’s claims and of the Defendants’ incentive and capacity to hide their misconduct. Indeed, the record already establishes that Awad directed Leviloff to lie about his true intentions of leaving the company and that Leviloff lied to his Middesk coworker about why he needed to receive certain of the confidential documents. *See Ayyash*, 233 F.R.D. at 327; *see also Suber v. VVP Servs.*, No. 20-8177, 2021 WL 1101235, at *10 (S.D.N.Y. Mar. 23, 2021) (ordering expedited discovery when plaintiff made a strong showing of the substantiality of claims that parties acted in a coordinated manner in furtherance of a fraud scheme). The record referenced above is supported by Defendants’ own words in secret text messages and supported by a detailed forensic examination report showing that Defendants obtained confidential information and trade secrets and that they stored that information on personal and/or Baselayer devices and other sources. These facts easily establish good cause for expedited discovery.

B. Even Though the Court Need Not Consider Them, the *Notaro* Factors Also All Weigh in Favor of Granting Middesk’s Motion.

Even if the Court considered the old four-factor *Notaro* test, which does not apply any more, *Stern*, 246 F.R.D. at 457, all those factors also strongly support expedited discovery.

Irreparable injury. Irreparable harm is presumed where trade secrets have been misappropriated because a “trade secret once lost is, of course, lost forever.” *FMC Corp. v. Taiwan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir. 1984). Here, the information in question is of great

value to Middesk as it relates to its business strategy and methodologies, and the “loss of trade secrets cannot be measured in money damages.” *Id.* In addition, even “where a trade secret has not yet been disclosed, irreparable harm may be found” where “trade secrets will inevitably be disclosed” and “the movant competes directly” with the new employer and the “transient employee possesses highly confidential or technical knowledge.” *Estee Lauder Cos. v. Batra*, 430 F. Supp. 2d 158, 162, 174 (S.D.N.Y. 2006). Baselayer is a direct competitor of Middesk, and Awad and Leviloff’s digital footprints show that they both obtained confidential and highly sensitive information about Middesk’s business. This factor weighs strongly in favor of Middesk.

Some probability of success on the merits. Middesk is likely to prevail on the merits. The plain terms of the Awad Agreement and the Leviloff Agreement bar those individuals from disclosing Middesk’s confidential information and trade secrets outside the Company or from retaining it after termination. In addition, the Leviloff Agreement bars him from competing or preparing to compete against the Company. The text messages and other forensic evidence that Middesk has assembled, even just to date before filing this case, establish that Leviloff and Awad have breached their agreements with Middesk by disclosing and retaining confidential information and trade secrets outside of Middesk. The same misconduct makes Middesk likely to prevail on its related claims. Furthermore, this misconduct coupled with the forensic IT report from Middesk’s expert makes it likely that this misconduct is just the tip of the iceberg and that Defendants were able to improperly capture additional Middesk information and misuse that for the benefit of themselves and Baselayer.

Some connection between the expedited discovery and the avoidance of irreparable injury. Courts routinely and appropriately order expedited discovery in cases like here where the plaintiff has alleged misappropriation of confidential information but does not yet know the extent to which

Defendants have exploited that information. *See, e.g., Sapient Corp. v. Singh*, 149 F. Supp. 2d 55, 57-58 (S.D.N.Y. 2001) (ordering expedited discovery after allegations that defendant formed a competing company and was using plaintiff's confidential information to solicit its clients); *IKON Office Solutions, Inc. v. Leichtnam*, No. 02-721, 2003 WL 251954, at *3 (W.D.N.Y. Jan. 3, 2003) (granting expedited discovery before injunction hearing where plaintiff had some evidence of former employee's misappropriation of confidential information and solicitation of plaintiff's customers on new employer's behalf). The expedited discovery that Middesk seeks here is tailored to establish the full extent of what Defendants stole and where it is. Because Middesk does not have independent access to all Defendants' devices and other sources where Defendants stored Middesk's confidential information and trade secrets, only by learning these details through discovery can Middesk seek to reduce or avoid further the irreparable injury it is suffering. This factor also strongly favors expedited discovery.

The injury that will result without expedited discovery is greater than the injury that the defendant will suffer if the expedited relief is granted. There is no injury that Defendants' will suffer from expedited discovery because the purpose is to discover the extent and whereabouts of Middesk's *own* confidential information and trade secrets. Nor can Defendants be heard to complain about any injury from being forced to refrain from possessing or using confidential information and trade secrets from Middesk to which Defendants had no right in the first place. Moreover, because the requested expedited discovery is proper and relevant, its discoverability is only a matter of timing: Defendants will inevitably have to produce this information in this case. There is no injury or prejudice to Defendants in being required to produce that information now. *See N. Atl. Operating Co.*, 293 F.R.D. at 370 ("Discovery inherently places a burden on the

responding party, but in this case, that hardship is outweighed by the harm that may result to [Middesk] if [its] request is denied.”).

By contrast, Middesk would suffer significant injury by not receiving expedited discovery. Middesk would not know all the documents and information that Defendants’ stole, would not know where its own confidential information and trade secrets were (other than to know they are in the hands of its competitor), and would not know how Defendants were improperly using that information. Moreover, given the ease with which Defendants lied to Middesk to obtain the confidential information and trade secrets in the first place, a Court order for expedited discovery and forensic imaging is needed to preserve a fair record on which to litigate the forthcoming preliminary injunction motion and the rest of this case. Here, the evidence subject to expedited discovery resides with the Defendants, and they have incentive and capacity to conceal it. As a result, this factor also strongly weighs in favor of Middesk.

All the *Notaro* factors, favor granting Middesk’s motion.

C. The Expedited Discovery Middesk Seeks Is Reasonable and Tailored.

The expedited discovery that Middesk seeks here is narrow, reasonably tailored, and appropriate given the brazen and extraordinary intrusion into Middesk’s confidential information and trade secrets orchestrated by its business competitor.

1. Middesk Seeks a Small Number of Document Requests, Interrogatories, and Depositions.

Courts routinely authorize parties to serve document requests and interrogatories and take depositions as expedited discovery in trade secret and restrictive covenant disputes. *See, e.g., Russell Reynolds Assocs., Inc. v. Usina*, No. 23-2369, 2023 WL 3270344, at *2 (S.D.N.Y. May 5, 2023) (allowing depositions, document requests, and interrogatories as expedited discovery in restrictive-covenant dispute); *R.R. Donnelley & Sons Co. v. Marino*, 505 F. Supp. 3d 194, 210

(W.D.N.Y. 2020) (ordering expedited deposition and document discovery in trade-secret dispute).

Accordingly, the Court should grant Middesk's request to serve document requests and interrogatories and to depose the three Defendants.

Middesk requests that the Court order Defendants to respond to the following expedited discovery requests within five days of the Court's Order and for each Defendant to be deposed within 21 days after the Defendants' expedited production:

Document Requests

- | | |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| To Awad: | <ol style="list-style-type: none"> 1. All documents about or communications with Leviloff since January 1, 2025 relating to Middesk, Baselayer, or Middesk Documents or Information. "Middesk Documents or Information" means any document drafted by Middesk, with Middesk metadata in it, or containing Middesk's confidential or proprietary information and/or trade secrets.
 2. All "Middesk Documents or Information" in your possession, custody or control. |
| To Leviloff: | <ol style="list-style-type: none"> 1. All documents about or communications with Awad since January 1, 2025 relating to Middesk, Baselayer, or Middesk Documents or Information.
 2. All "Middesk Documents or Information" in your possession, custody or control.
 3. All documents about or communications with Baselayer or any Baselayer employee or agent from September 1, 2024 until you began full-time employment at Baselayer. |
| To Baselayer: | <ol style="list-style-type: none"> 1. All documents and communications about (i) Leviloff's transition to and exit from Baselayer, including but not limited to any investigation of his conduct and his personnel file, or (ii) Leviloff's work at Middesk or knowledge of Middesk's confidential information or trade secrets.
 2. All documents or communications about (i) Middesk Documents or Information or requesting Middesk Documents or Information or (ii) soliciting Middesk employees, including Leviloff, or trying to obtain Middesk confidential information or trade secrets.
 3. All "Middesk Documents or Information" in your possession, custody or control and all communications about "Middesk Documents or Information." |

Interrogatories

- To Awad:
1. Identify all business and personal devices, cloud storage, email or cell phone accounts, and other data sources used by Awad since January 1, 2025.
 2. Identify and describe all attempts to and instances of requesting or receiving Middesk Documents or Information from Middesk or its current or former employees, whether from Leviloff or otherwise.
- To Leviloff:
1. Identify all business and personal devices, cloud storage, email or cell phone accounts, and other data used by Leviloff since September 1, 2024.
 2. Identify and describe all requests by any third party or instances by you of providing Middesk Documents or Information to a third party, to yourself, or to a device or data source you possess or control, including but not limited to involving Awad.
- To Baselayer:
1. Identify all devices, cloud storage, email or cell phone accounts, or other data sources issued to or used by Awad or Leviloff for Baselayer business since January 1, 2025.
 2. Identify all Baselayer employees who communicated with Leviloff since January 1, 2025 and, for each such Baselayer employee, identify all their Baselayer devices, email accounts, and systems/cloud storage they had access to.
 2. Middesk Seeks a Forensic Examination of Specifically Identified Devices/Sources.

Middesk also seeks a tailored forensic examination of certain of Defendants' devices/data sources that Middesk's forensic IT expert has determined were involved in the scheme to steal Middesk's confidential information and trade secrets. After a thorough investigation of the available materials, Middesk's expert has identified specific devices and other data sources that Middesk needs to examine to learn the full extent of what Defendants took and where it now resides. *See infra* at 21-22.

Courts frequently order forensic examinations in connection with expedited discovery because “[q]uickly determining what information Defendant removed from Plaintiff, and whether

and how Plaintiff's information is being used by Plaintiff's competitors is essential in order to minimize any harm to Plaintiff's competitive position.”³ Even if some courts construe forensic examinations as a less routine form of relief, the well-documented extraordinary intrusion into Middesk's confidential information and trade secrets here, plus Middesk's expert's identification of specific devices/sources likely to contain that information, warrant that relief. The burden on Defendants is minimal, as all Middesk requests is access to Defendants' devices. *See Synopsys, Inc. v. InnoGrit, Corp.*, No. 19-2082, 2019 WL 1779978, at *4 (N.D. Cal. Apr. 23, 2019).

For example, in *Citibank, N.A. v. Mitchell*, the Court ordered forensic discovery in a case against former Citi employees in which just two days before giving notice of their resignation to move to a competitor, the employees accessed Citi's confidential client information.⁴ The employees' search of Citi records included client lists and clients' cash balances and even included

³ *Citibank, N.A. v. Mitchell*, 2024 WL 4906076, at *7 (N.D. Cal. Nov. 26, 2024) (ordering forensic computer examination of any electronic devices that have stored, accessed, or transmitted plaintiff's trade secret or confidential or proprietary information as part of expedited discovery); *IME Watchdog, Inc. v. Safa Abdulrahim Gelardi, et. al.*, No. 22-cv-1032, slip op. at ECF No. 66, at 18 (E.D.N.Y. May 13, 2022) (ordering defendant to provide “complete and unrestricted access to their records and electronic accounts to the forensic analyst” in a trade secret case); *Campbell Alliance Grp., Inc. v. Dandekar*, No. 13-415, 2013 WL 12144048, at **2, 4 (E.D.N.C. Dec. 23, 2013) (ordering “forensic examination of any computers and/or electronic devices on which plaintiff's confidential and proprietary information may be located” in a restrictive covenant dispute); *Ceglia v. Zuckerberg*, No. 10-569, 2013 WL 1208558, at *1, 5 (W.D.N.Y. March 26, 2013) (noting that expedited discovery, including forensic examination, was ordered to determine whether documents were forged in contract dispute); *Pyro Spectaculars North, Inc. v. Souza*, 2012 WL 13220023, at *3 (E.D. Cal. Feb. 8, 2012) (ordering forensic examination of defendant's and wife's computers and electronic storage media within six days of the Order as part of expedited discovery); *PLC Trenching Co., LLC v. Newton*, 2011 WL 13135653, at *13 (N.D.N.Y. 2011) (allowing plaintiff to inspect and perform a forensic investigation of Defendants' computer systems to ensure that Defendants are not retaining and exploiting plaintiff's patents in trade secret misappropriation case)

⁴ 2024 WL 4906076, at *2.

a search on Citi’s system for “my clients.”⁵ The Court found that the client information searched included information that the defendant “had not recently accessed.”⁶

The facts here are even worse and easily justify a forensic examination. Like in *Citibank*, Leviloff accessed Middesk confidential information that he had not recently accessed shortly before he left the Company to join a competitor. But, even worse, Leviloff did so at the express direction of that competitor’s CEO and lied to his Middesk colleague to receive information to which Leviloff was not privy in his day-to-day duties. Only forensic analysis of Awad’s and Leviloff’s personal and Baselayer devices will show what information was actually removed and “whether and how [it] is being used by [Baselayer]” to Middesk’s detriment.⁷ Middesk cannot obtain a full accounting of Defendants’ actions in connection to its trade secrets in any other way. Middesk needs a forensic examination of Leviloff’s phone and cloud storage to determine the full extent of what they took, where they subsequently sent it, and how they used it. If Defendants maintain that this search is intrusive, only they are to blame for downloading confidential information and trade secrets of their former employer, orchestrating this scheme, and importing Middesk’s confidential information and trade secrets into the company and/or personal devices and other sources that they did. Accordingly, these facts favor forensic examination of the identified devices and other sources at this stage.

⁵ *Id.*

⁶ *Id.*

⁷ *Comet Techs. United States of Am. Inc. v. Beuerman*, No. 18-CV-01441-LHK, 2018 WL 1990226, at **1, 7 (N.D. Cal. Mar. 15, 2018) (ordering expedited discovery so plaintiff can determine “current location” of trade secrets after defendant removed confidential information from former employer and in the process searched “website detailing how to prevent others from ‘Find[ing] out what searches you did or sites you visited’ and from ‘See[ing] that your account was signed in.’”).

Middesk's expert has already identified the list of devices and other data sources not in Middesk's possession that Ackert would need to complete his IT forensics investigation:

- Leviloff's Gmail account: JXXXXXXXXXX@gmail.com;
- Leviloff's iCloud account associated with the email address jXXXXXXXXXX@yahoo.com;
- Leviloff's personal phone;
- Leviloff's personal computer(s);
- Leviloff's Baselayer-provided computer;
- Leviloff's Baselayer-provided email account;
- Awad's Apple ID associated with email account j*****@gmail.com, including the full email address and password;
- Awad's device(s) used to communicate with Leviloff;
- Awad's Baselayer-provided computer;
- Awad's Baselayer-provided email account; and
- Baselayer accounts or systems that Leviloff connected to or emailed. *See* Ackert Decl. ¶ 65.

That list is the product of a reasoned and thorough forensic investigation, and the Court should order this discrete list of devices and data sources to be imaged to preserve the record and allow Middesk to have full and fair access to the evidence in preparing for the forthcoming preliminary injunction hearing. Middesk agrees to initially cover the cost of the forensic examination, subject to Middesk's ability to seek to recover those costs as additional damages in this litigation.

III. CONCLUSION

For the foregoing reasons, Plaintiffs' respectfully requests that this Court grant the proposed Order to Show Cause. Specifically, Middesk requests that the Court:

- (1) order Defendants to make a complete production of documents and fully respond to the interrogatories within five (5) days of the entry of the Court's Order (the "Expedited Production");
- (2) order that Defendants make available the devices/data sources of information at the time of the Expedited Production so Middesk's vendor can forensically image those sources;

- (3) allow Middesk to depose each defendant for three hours or less for purposes of a forthcoming preliminary injunction hearing within 21 days after the Expedited Production; and
- (4) set a hearing date and briefing schedule for a preliminary injunction in favor of Middesk.

Middesk respectfully asks the Court to consider this Motion and order any response by Defendants on an expedited basis.

Dated: March 31, 2025

Respectfully submitted,
/s/ Jason D. Burns
Jason D. Burns
Shira M. Poliak
GREENBERG TRAURIG, LLP
One Vanderbilt Avenue
New York, NY 10017
(212) 801-9294
Jason.Burns@gtlaw.com
Shira.Poliak@gtlaw.com

Justin K. Victor (*phv forthcoming*)
Fredric J. Bold, Jr. (*phv forthcoming*)
Rushton Pope (*phv forthcoming*)
GREENBERG TRAURIG, LLP
3333 Piedmont Road NE, Suite 2500
Atlanta, GA 30305
(678) 553-2100
victorj@gtlaw.com
rick.bold@gtlaw.com
rushton.pope@gtlaw.com

Counsel for Plaintiff

CERTIFICATION OF COMPLIANCE WITH THE WORD LIMIT

Pursuant to Local Civil Rule 7.1, Plaintiff Middesk, Inc. states that its Memorandum of Law In Support of Order to Show Cause for Expedited Discovery, filed on March 31, 2025, complies with the 8,750 word limit. The memorandum of law is 6,702 words.